New Android banking malware remotely takes control of your device

bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/

Bill Toulas

By
Bill Toulas

- April 9, 2022
- 11:02 AM
- 1

A new Android banking malware named Octo has appeared in the wild, featuring remote access capabilities that allow malicious operators to perform on-device fraud.

Octo is an evolved Android malware based on ExoCompact, a malware variant based on the Exo trojan that quit the cybercrime space and had its source code leaked in 2018.

The new variant has been discovered by researchers at ThreatFabric, who observed several users looking to purchase it on darknet forums.

On-device fraud capabilities

Octo's significant new feature compared to ExoCompact is an advanced remote access module that enables the threat actors to perform on-device fraud (ODF) by remotely controlling the compromised Android device.

The remote access is provided through a live screen streaming module (updated every second) through Android's MediaProjection and remote actions through the Accessibility Service.

Octo uses a black screen overlay to hide the victim's remote operations, sets screen brightness to zero, and disables all notifications by activating the "no interruption" mode.

By making the device appear to be turned off, the malware can perform various tasks without the victim knowing. These tasks include screen taps, gestures, text writing, clipboard modification, data pasting, and scrolling up and down.

On-Device Fraud allows complete takeover of the compromised device
Source: ThreatFabric

Apart from the remote access system, Octo also features a powerful keylogger that can monitor and capture all victims' actions on infected Android devices.

This includes entered PINs, opened websites, clicks and elements clicked, focus-changing events, and text-changing events.

Finally, Octo supports an extensive list of commands, with the most important being:

- Block push notifications from specified applications
- Enable SMS interception
- Disable sound and temporarily lock the device's screen

- Launch a specified application
- Start/stop remote access session
- Update list of C2s
- Open specified URL
- Send SMS with specified text to a specified phone number

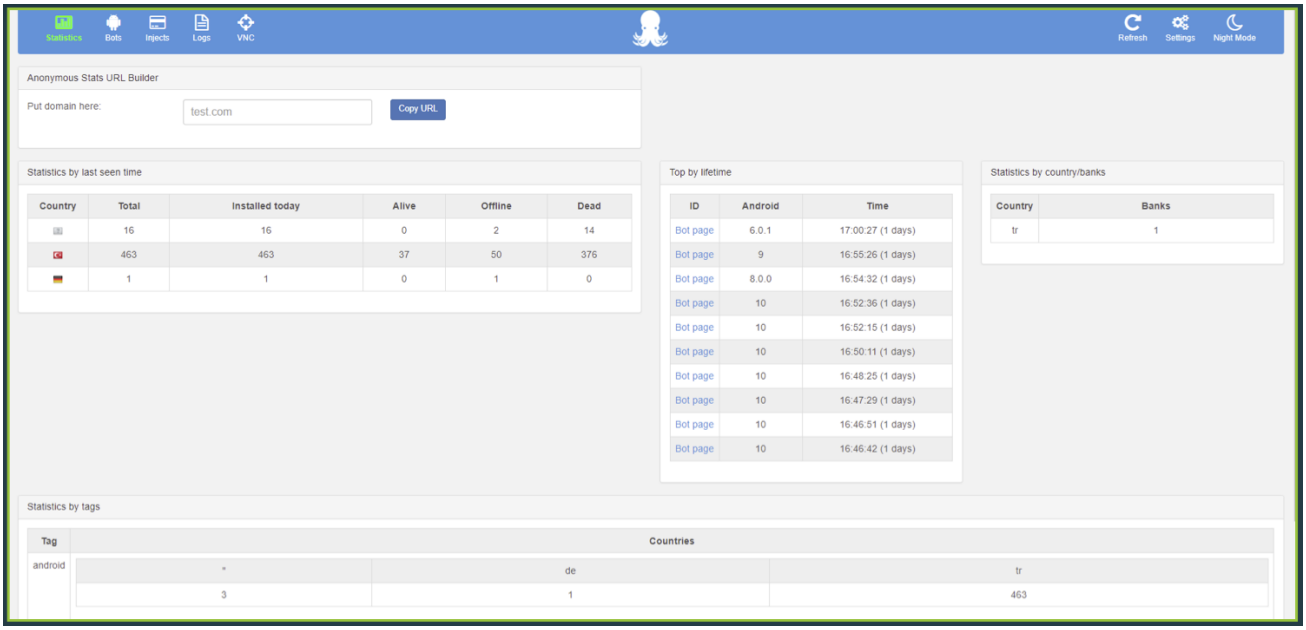
Campaigns and attribution

Octo is sold on forums, such as the Russian-speaking XSS hacking forum, by a threat actor using the alias "Architect" or "goodluck."

Of particular note, while most posts on XSS are in Russian, almost all posts between Octo and potential subscribers have been written in English.

Due to the extensive similarities with ExoCompact, including Google Play publication success, Google Protect disabling function, and the reverse engineering protection system, ThreatFabric believes there's a good chance that 'Architect' is either the same author or a new owner of ExoCompact's source code.

ExoCompact also features a remote access module, albeit a simpler one, also provides command execution delay options and has a similar admin panel to Octo's.

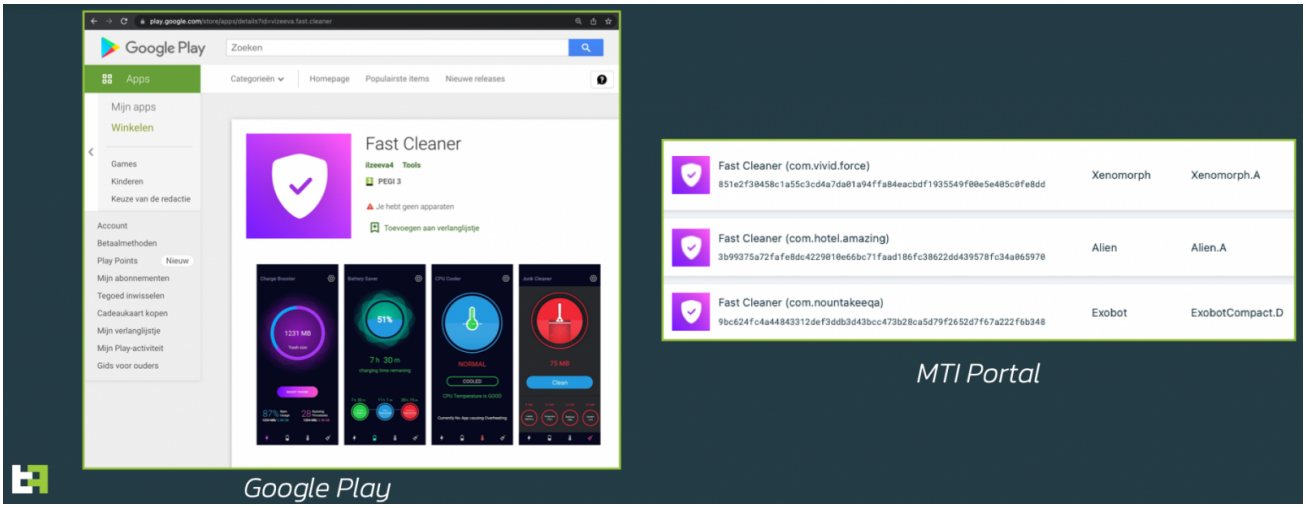


Octo's panel

Source: ThreatFabric

"Thus, having these facts in mind, we conclude that ExobotCompact was rebranded to Octo Android banking Trojan and is rented by its owner "Architect", also known as "goodluck". ThreatFabric tracks this variant as ExobotCompact.D," concludes Threat Fabric in their report.

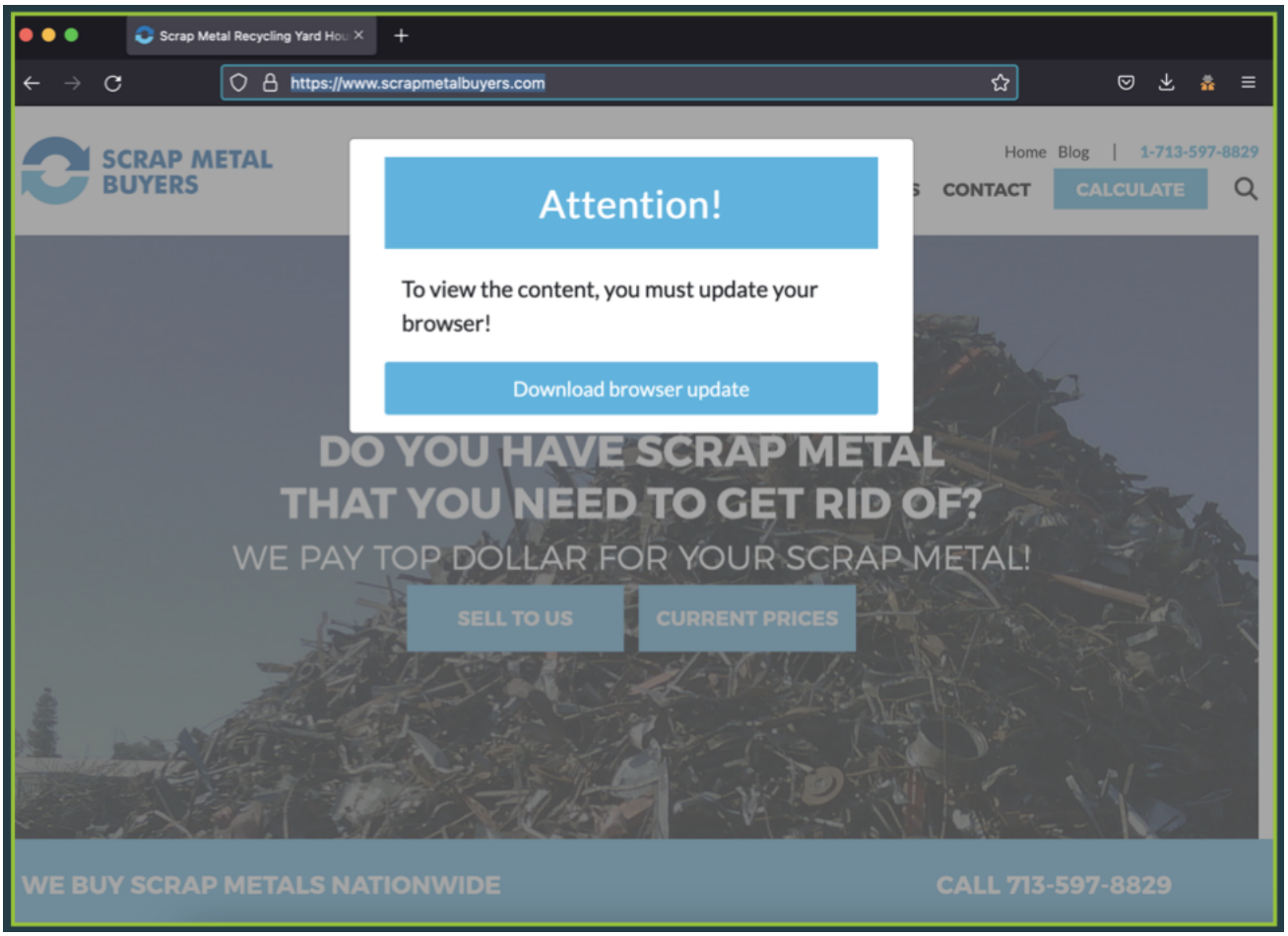
Recent Google Play apps that infected devices with Octo include an app named "Fast Cleaner," which had 50,000 installs until February 2022, when it was discovered and removed.



Fast Cleaner app delivering Octo to victims

Source: ThreatFabric

Other Octo campaigns relied on sites using fake browser update notices or bogus Play Store app update warnings.



Fake browser update notice pushing Octo installers

Source: ThreatFabric
Some Octo operators managed to infiltrate the Play Store again after the Fast Cleaner operation was over, using an app named "Pocket Screencaster."

The full list of known Android apps containing the Octo malware is listed below:

- Pocket Screencaster (com.moh.screen)
- Fast Cleaner 2021 (vizeeva.fast.cleaner)
- Play Store (com.restthe71)
- Postbank Security (com.carbuildz)
- Pocket Screencaster (com.cutthousandjs)
- BAWAG PSK Security (com.frontwonder2), and
- Play Store app install (com.theseeye5)

A dangerous new breed

Trojans featuring remote access modules are becoming more common, rendering robust account protection steps such as two-factor codes obsolete as the threat actor completely controls the device and its logged-in accounts.

Anything the user sees on their device's screen becomes within the access of these malware variants, so after infection, no information is safe, and no protection measure is effective.

That said, users need to remain vigilant, keep the number of apps installed on their smartphones at a minimum, and regularly check to ensure Play Protect is enabled.

Related Articles:

Top 10 Android banking trojans target apps with 1 billion downloads

SMSFactory Android malware sneakily subscribes to premium services

Mobile trojan detections rise as malware distribution level declines

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

New stealthy Nerbian RAT malware spotted in ongoing attacks

- Android
- Banking Trojan
- Exobot
- Octo
- Remote Access Trojan
- Trojan

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Comments

ANTP - 2 months ago

-
-

Scary!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: